(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 August 2003 (07.08.2003)

PCT

(10) International Publication Number
WO 03/065723 A3

(51) International Patent Classification[7]: H04N 7/16

(21) International Application Number: PCT/IB03/00214

(22) International Filing Date: 20 January 2003 (20.01.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02075418.0 1 February 2002 (01.02.2002) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BRUEKERS, Alphons, A., M., L.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **MAANDONKS, Arnoldus, J., L., M.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **MITTERTREINER, Peter-Paul** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **VERBRUGGEN, Johannes, F., E., M.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: **GROENENDAAL, Antonius, W., M.**; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

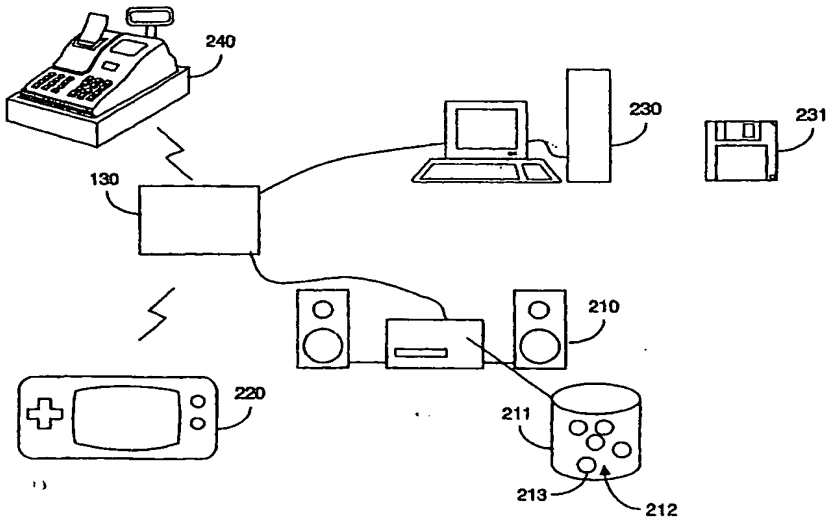
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**
— *with international search report*

(88) Date of publication of the international search report:
13 November 2003

*[Continued on next page]*

(54) Title: WATERMARK-BASED ACCESS CONTROL METHOD AND DEVICE




(57) Abstract: A method of controlling access to a resource (140) using a verifying device (130). A watermarking device (110) embeds an authorization code in a signal (120) using watermarking technology. The watermarked signal (120) is then transmitted to a verifying device (130), e.g. as a television or radio program or as a commercial related to the resource (140). In the verifying device (130), the authorization code is extracted from the watermarked signal (120) and an operation to be performed on the resource (140) is authorized in dependence on the extracted authorization code. Preferably the authorization comprises permission for executing a program (231), rendering and/or copying a multimedia object (213) or for activating a cheat function in an electronic game (220).

WO 03/065723 A3

THIS PAGE BLANK (USPTO)

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 03/00214

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F A63F H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 2001/026618 A1 (VAN WIE DAVID M ET AL)<br>4 October 2001 (2001-10-04)<br>abstract<br>paragraphs '0044!,'0045!<br>paragraph '0047!<br>paragraphs '0051!,'0052!<br>paragraphs '0072!-'0077!<br>paragraph '0087!<br>paragraph '0104! | 1,5,6,<br>10,11,13 |
| X | US 5 710 815 A (MING ET AL)<br>20 January 1998 (1998-01-20)<br>column 6, line 43 - line 47<br>column 5, line 67 -column 6, line 5<br>column 2, line 56 - line 59<br>column 2, line 11 - line 12<br>abstract | 1,5,10 |

-/—

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 21 August 2003 | 29/08/2003 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Dockhorn, H |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Internatic plication No
PCT/IB 03/00214

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | WO 99 48296 A (INTERTRUST TECHNOLOGIES CORP) 23 September 1999 (1999-09-23)<br>abstract<br>page 7, line 23 - line 25 | 1,5,10 |
| X | US 5 862 260 A (RHOADS GEOFFREY B)<br>19 January 1999 (1999-01-19)<br>column 1, line 35 - line 40<br>column 27, line 25 - line 41 | 1,10 |
| A | US 5 971 855 A (NG VICTOR)<br>26 October 1999 (1999-10-26)<br>column 2, line 47 - line 51 | 1,4,10 |

# INTERNATIONAL SEARCH REPORT

Internatio ɔlication No
PCT/IB 03/00214

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2001026618 A1 | 04-10-2001 | US 6240185 B1 | 29-05-2001 |
| | | US 5943422 A | 24-08-1999 |
| | | US 2003002673 A1 | 02-01-2003 |
| | | AU 3205797 A | 05-12-1997 |
| | | AU 739300 B2 | 11-10-2001 |
| | | AU 3681697 A | 19-02-1998 |
| | | CN 1225739 A | 11-08-1999 |
| | | EP 0898777 A2 | 03-03-1999 |
| | | JP 2001501763 T | 06-02-2001 |
| | | WO 9743761 A2 | 20-11-1997 |
| US 5710815 A | 20-01-1998 | AU 6329196 A | 30-12-1996 |
| | | WO 9641438 A1 | 19-12-1996 |
| WO 9948296 A | 23-09-1999 | CA 2323781 A1 | 23-09-1999 |
| | | CA 2425741 A1 | 23-09-1999 |
| | | CN 1301459 T | 27-06-2001 |
| | | EP 1062812 A1 | 27-12-2000 |
| | | JP 2002507868 T | 12-03-2002 |
| | | WO 9948296 A1 | 23-09-1999 |
| US 5862260 A | 19-01-1999 | US 5832119 A | 03-11-1998 |
| | | US 5748783 A | 05-05-1998 |
| | | US 5768426 A | 16-06-1998 |
| | | AU 3008697 A | 05-12-1997 |
| | | EP 1019868 A2 | 19-07-2000 |
| | | US 2002090113 A1 | 11-07-2002 |
| | | US 2002136429 A1 | 26-09-2002 |
| | | WO 9743736 A1 | 20-11-1997 |
| | | US 2002164049 A1 | 07-11-2002 |
| | | US 2002186886 A1 | 12-12-2002 |
| | | US 2002188841 A1 | 12-12-2002 |
| | | US 2002186887 A1 | 12-12-2002 |
| | | US 2003012403 A1 | 16-01-2003 |
| | | US 2003021441 A1 | 30-01-2003 |
| | | US 2003031341 A1 | 13-02-2003 |
| | | US 2003033530 A1 | 13-02-2003 |
| | | US 2003091189 A1 | 15-05-2003 |
| | | US 2003039377 A1 | 27-02-2003 |
| | | US 2003053653 A1 | 20-03-2003 |
| | | US 2003053654 A1 | 20-03-2003 |
| | | US 2003102660 A1 | 05-06-2003 |
| | | US 2003086585 A1 | 08-05-2003 |
| | | US 2003142847 A1 | 31-07-2003 |
| | | US 2003128861 A1 | 10-07-2003 |
| | | US 2003103645 A1 | 05-06-2003 |
| | | US 2003133592 A1 | 17-07-2003 |
| | | US 6307949 B1 | 23-10-2001 |
| | | US 6381341 B1 | 30-04-2002 |
| | | US 6408082 B1 | 18-06-2002 |
| | | US 6553129 B1 | 22-04-2003 |
| | | US 6567533 B1 | 20-05-2003 |
| | | US 6505160 B1 | 07-01-2003 |
| | | US 6424725 B1 | 23-07-2002 |
| | | US 6122403 A | 19-09-2000 |
| | | US 2001031065 A1 | 18-10-2001 |
| | | US 2001022848 A1 | 20-09-2001 |
| | | US 2001019618 A1 | 06-09-2001 |

# INTERNATIONAL SEARCH REPORT

International application No
PCT/IB 03/00214

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 5862260 A | | US 2001055407 A1 | 27-12-2001 |
| | | US 2001017931 A1 | 30-08-2001 |
| | | US 2001016051 A1 | 23-08-2001 |
| | | US 2002009208 A1 | 24-01-2002 |
| | | US 2002006212 A1 | 17-01-2002 |
| | | US 2002067844 A1 | 06-06-2002 |
| | | US 2002118831 A1 | 29-08-2002 |
| | | US 2002076081 A1 | 20-06-2002 |
| | | US 2002090112 A1 | 11-07-2002 |
| | | US 2002080997 A1 | 27-06-2002 |
| | | AU 6022396 A | 29-11-1996 |
| | | CA 2218957 A1 | 14-11-1996 |
| | | EP 1003324 A2 | 24-05-2000 |
| US 5971855 A | 26-10-1999 | AU 9676898 A | 23-04-1999 |
| | | WO 9916520 A1 | 08-04-1999 |

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 August 2003 (07.08.2003)

PCT

(10) International Publication Number
WO 03/065723 A2

(51) International Patent Classification[7]: H04N 7/16

(21) International Application Number: PCT/IB03/00214

(22) International Filing Date: 20 January 2003 (20.01.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02075418.0 1 February 2002 (01.02.2002) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BRUEKERS, Alphons, A., M., L.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **MAANDONKS, Arnoldus, J., L., M.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **MITTERTREINER, Peter-Paul** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **VERBRUGGEN, Johannes, F., E., M.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

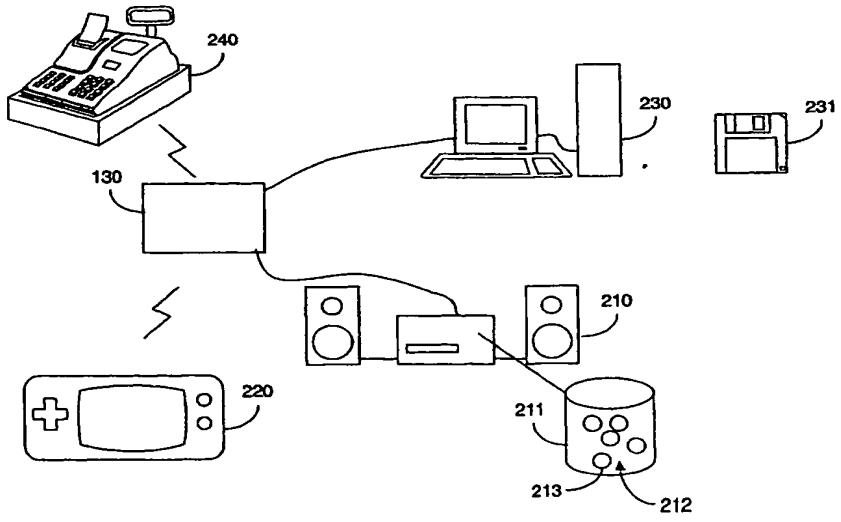
(74) Agent: **GROENENDAAL, Antonius, W., M.**; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

*[Continued on next page]*

(54) Title: WATERMARK-BASED ACCESS CONTROL METHOD AND DEVICE




(57) Abstract: A method of controlling access to a resource (140) using a verifying device (130). A watermarking device (110) embeds an authorization code in a signal (120) using watermarking technology. The watermarked signal (120) is then transmitted to a verifying device (130), e.g. as a television or radio program or as a commercial related to the resource (140). In the verifying device (130), the authorization code is extracted from the watermarked signal (120) and an operation to be performed on the resource (140) is authorized in dependence on the extracted authorization code. Preferably the authorization comprises permission for executing a program (231), rendering and/or copying a multimedia object (213) or for activating a cheat function in an electronic game (220).

WO 03/065723 A2

**Published:**
— *without international search report and to be republished upon receipt of that report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

# Watermark-based access control method and device

The invention relates to a method of controlling access to a resource such as a computer program or a multimedia object. The invention further relates to a verifying device arranged for controlling access to a resource.

Watermarking, the process of inserting extra information in a signal such as an audio or video signal, is an important and well-known technique to mark or protect those signals. A movie can be watermarked so its origin can be identified, or unauthorized copies can be distinguished from the original. Watermarks can be used with still images to locate copies reproduced by unauthorized third parties, by simply downloading images from the information services offered by those third parties and examining the downloaded images for the watermark.

Watermarks can also be used to embed metadata, such as an Internet Uniform Resource Locator (URL), in the input signal, for instance in a movie. Upon receiving a signal with the embedded extra information, a device can decode the URL and fetch the associated resource for displaying it to the user. A user who views the movie at his personal entertainment station can thus access the embedded metadata to access, for instance, the World-Wide Web site of the movie.

International patent application PCT/EP01/12712 (attorney docket PHNL000591) by the same applicant as the present application describes how a command can be transmitted to a controllable device by embedding it using watermarking techniques in a signal like a television program or a piece of music. A watermark detector in the controllable device picks up the signal, preferably through the acoustical domain, detects the watermarked command and executes it. The controllable device is preferably embodied as a toy, which can then be controlled to "play along" with a children's television program.

In another application of watermarking, rights regarding the copying and/or playback of a multimedia object like a movie or song are embedded in the multimedia object using watermarking technology. A playback or copying apparatus can then extract these

rights from the multimedia object and operate in accordance with the extracted rights, e.g. by refusing to copy the multimedia object if no copying rights are embedded in the object.

However, this application of watermarking suffers from the drawback that the rights embedded in the multimedia object cannot be easily modified. This makes it difficult to later provide additional rights, or to revoke previously granted rights for the multimedia object.

It is an object of the invention to provide a method according to the preamble, which provides a flexible way to authorize operations on the resource.

This object is achieved according to the invention in a method comprising embedding an authorization code in a signal by means of a watermark and transmitting the watermarked signal to a verifying device, and in the verifying device, extracting the authorization code from the watermarked signal and authorizing an operation to be performed on the resource in dependence on the extracted authorization code.

By embedding the authorization code using watermarks in a signal, the authorization codes can be supplied to the verifying device without the need for special communication channels between an entity supplying authorization and the verifying device. In effect, the normally available audio and/or video transmission channels are used to supply authorization codes to the verifying device. Further, new authorization codes, as well as revocations for previously supplied authorization codes, can easily be supplied by embedding them in subsequent signals transmitted in the same way.

The signal in which the authorization code is embedded does not represent the resource to which the authorization code applies. Rather, the signal is merely used as a carrier for getting the authorization code to the verifying device controlling access to the resource.

In an embodiment the resource comprises a computer program and the authorization code causes the verifying device to grant permission for executing the program. Execution of programs can be controlled using so-called license managers. License managers are computer programs that control the execution of other programs based on license codes. Ordinarily these license codes have to be purchased from a supplier and entered into the license manager software to enable execution of the programs under its control. In this embodiment the license code is supplied as an authorization code embedded in a signal, making it possible to automatically extract the license code and supply it to the license

manager. The license manager will then allow a user to execute the computer program based on the license code.

In a further embodiment the resource comprises a computer program and the authorization code causes the verifying device to grant permission for activating a module of the computer program. One way to promote a computer program is to distribute a so-called "shareware" version, in which part of the functionality is disabled. This allows potential buyers of the program to try it out for free. As the disabled functions can be seen but not used, users of the shareware version are encouraged to buy the whole program.

Typically buying the full version of a program is done by purchasing a license code that is to be entered in the shareware program. If the right code is entered, the disabled modules are enabled and the full functionality becomes available. This embodiment of the invention makes it possible to enable such a disabled module using a license code embedded in a signal such as a commercial promoting the computer program, or a television program reviewing the program.

In a further embodiment the resource comprises an electronic game and the authorization code causes the verifying device to grant permission for activating a cheat function in the electronic game. A cheat code allows the player of an electronic game to access functionality of the game that would normally not be accessible. For example, the player's character could be invincible in the game for a certain time, receive extra points or weapons, and so on.

Normally, such cheat codes are distributed as alphanumerical strings or sequences of buttons to be pressed ("press left-left-up-right-escape to become invincible"). In this embodiment the authorization code provides a cheat code for use in the electronic game. This makes it much easier for the player to activate the cheat function. The authorization code could be embedded in a television program related to electronic games. This encourages players to watch the television program because they want to obtain the cheat codes.

In a further embodiment the resource comprises a multimedia object and the authorization code causes the verifying device to grant permission for at least one of: a rendering of the multimedia object and the making of a copy of the multimedia object. Digital rights management (DRM) systems can be used to enforce restrictions on rendering and/or copying of multimedia objects. This forces people to obtain "rights" or permissions for rendering and/or copying. The present invention makes it possible to grant these "rights" by embedding them in signals likely to be received by verifying devices coupled to DRM systems.

The signal could e.g. represent an advertisement related to the multimedia object. If, after hearing the advertisement a user receives a (preferably one-time) playback right for a multimedia object, he will be greatly encouraged to also view future advertisements, and to buy the advertised product, which will typically be an item like a record carrier comprising the multimedia object or a concert by the artist performing the multimedia object.

Preferably, in the above embodiments the permission is limited in time. This way, the effect of the permission can be limited to a certain time period. It also realizes a greater audience for entities transmitting the watermarked signals, such as television broadcasters, radio stations and so on, as people wishing to make use of the authorization codes now must obtain these codes before the limited time expires.

In a further embodiment the resource comprises a computer program and the authorization code causes the verifying device to revoke a previously granted permission for executing the program. This makes it possible to distribute programs that are only supposed to be executed for a limited time, such as beta or test versions of a program.

In a variant of this embodiment the authorization code further causes the verifying device to authorize a further operation to be performed on the resource. It is to be expected that users will try to avoid receiving authorization codes that revoke previously granted permissions. One way to overcome this problem is to provide a positive authorization together with the revocation.

For example, if the authorization code revokes permission to execute a beta version of a computer program, it could at the same time grant permission to execute the official release version of that computer program. This way a beta tester is encouraged to allow revocation of the beta version. Preferably this further authorization is delayed until a predetermined time has elapsed after the revocation took place.

In a further embodiment the signal comprises an advertisement related to the resource. This has the advantage that a person listening to or viewing the signal can easily associate any authorizations granted by the embedded authorization codes with resources to which the authorizations apply. Further, it encourages the viewing or listening to advertisements.

It is a further object of the invention to provide a verifying device according to the preamble, which is capable of handling authorizations in a flexible matter.

This object is achieved according to the invention in a verifying device comprising receiving means for receiving a watermarked signal, watermark detection means

for detecting an authorization code embedded in the watermarked signal, and access control means for authorizing an operation to be performed on the resource in dependence on the extracted authorization code.

A very flexible channel is obtained by transporting the authorization code to the verifying device embedded in a watermark in a signal. If new, updated or otherwise modified authorization codes need to be supplied, or previously granted permissions need to be revoked, they can simply be embedded in a new signal transmitted to the verifying device. The verifying device does not need to have a special connection to any entity supplying authorization codes. It could simply tune in to broadcasted radio or TV signals, or detect watermarks in audio signals picked up using a microphone, and so on.

Thus, in terms of technical effects produced by the invention, the verifying device no longer needs a separate channel for receiving authorizations, can handle authorizations varying in time for one particular multimedia object without having to update the multimedia object, and can activate, modify or deactivate functionality in a resource like a computer.

In an embodiment the authorization code comprises a timestamp and the access control means are arranged for authorizing the operation further in dependence on a comparison of the timestamp against a current time. This way the access control means can determine the validity of the extracted authorization code. The access control means can then ignore authorization codes extracted after the end of a validity period indicated by the timestamp, and/or automatically revoke authorizations granted once the validity indicated by the timestamp expires.

The invention further relates to a computer program product arranged for causing a general purpose computer to function as the verifying device of the invention.The invention further relates to a signal in which an authorization code is embedded by means of a watermark. Preferably the computer program product and/or the signal are embodied on a carrier such as a compact disc, a Digital Versatile Disc, a video tape or a floppy disc.

These and other aspects of the invention will be apparent from and elucidated with reference to the embodiments shown in the drawing, in which:

Fig. 1 schematically shows a system comprising a transmitter and a verifying device in accordance with the invention;

Fig. 2 schematically illustrates various applications of the method according to the invention.

Throughout the figures, same reference numerals indicate similar or corresponding features. Some of the features indicated in the drawings are typically implemented in software, and as such represent software entities, such as software modules or objects.

Fig. 1 schematically shows a system 100 comprising a watermarking device 110, a rendering device 114, a network 119 and a verifying device 130 configured to control access to a resource 140.

A receiving module 111 in the watermarking device 110 receives a content item, which is for instance a television program, a radio program, a movie, an advertisement or commercial, a picture or a sound or a portion thereof. It is usually received through a network such as the Internet, a satellite feed or a home network from a distributor 117 such as a television broadcasting organization. Alternatively, it can be loaded from local storage 118 which can be a tape or a disk such as a DVD or Video CD. It can also be a hard disk on which it has been previously recorded for later viewing.

In accordance with the invention, an authorizing module 112 determines an authorization code that is to be embedded in the content item. The authorization code can e.g. be obtained from an external source, be read from local storage 118 or be input by an operator of the watermarking device 110. A more detailed description of possible authorization codes and their uses can be found below with reference to Fig. 2.

An embedding module 113 embeds the authorization code in the content item, producing watermarked signal 120, using any kind of watermarking or other steganographic technique appropriate for the content 116. The watermarked signal 120 is then fed to rendering device 114 over a transmission medium 119, which can be e.g. a network such as the Internet, a satellite feed or a cable television network.

The rendering device 114 outputs the received signal 120 using audio output module 115 and/or video output module 116. If the signal 120 comprises audio and video signals, respective outputs may be synchronized with each other. In this embodiment the watermarked signal 120 is an audio signal, but it can equally well be a video signal. By rendering the watermarked signal 120 in this fashion, the verifying device 130 is able to receive it. Alternatively, the watermarked signal 120 could be transmitted directly to the

verifying device 130, for example using a network connection between the watermarking device 110 and the verifying device 130.

The verifying device 130 comprises receiving module 131, decoding module 132 and access control module 133. The receiving module 131 receives the watermarked audio signal 120 and feeds it to the decoding module 132. The receiving module 131 can be for instance a microphone, a camera or a light sensitive sensor of some kind.

The decoding module 132 processes the watermarked audio signal 120 to obtain the authorization code embedded therein. Detecting a watermark and extracting embedded information is well known in the art and will not be elaborated upon further. The authorization code is then fed to the access control module 133.

The access control module 133 is arranged to control access to a resource 140, which in the embodiment of Fig. 1 comprises a computer program running on a personal computer. In the context of computer programs, controlling access refers to things like granting permission for execution of the program, revoking a previously granted permission for execution of the program, granting permission for activation of a module of the program and so on. A user of the personal computer will be unable to execute the program or activate the module unless permission has been granted by the access control module 133. Ways for controlling access are discussed more extensively with reference to Fig. 2 below.

In accordance with the invention, the access control module 133 controls access to the resource 140 in dependence on the authorization code extracted from the watermarked signal 120 by the decoding module 132. This way, it is possible to grant or revoke permissions, or to otherwise control access to the resource 140, in a very flexible way by simply transmitting a new watermarked signal with an authorization code every time a new permission is to be granted or revoked.

The watermarking device 110 can be realized as a computer program product being arranged for causing a processor to execute the steps described above. The computer program product enables a programmable device when executing said computer program product to function as the watermarking device 110. Similarly, the verifying device 130 can be realized as a computer program product enabling a programmable device when executing said computer program product to function as the verifying device 130.

The above description gives a general overview of the functionality of distributing watermarked content. Various ways are possible to realize the watermarking device 110 and the verifying device 130, with different advantages and possibilities.

Fig. 2 schematically illustrates various applications of the method according to

the invention. The verifying device 130 is in Fig. 2 operably connected to a content playback apparatus 210, a gaming device 220, a personal computer 230, and a cash register 240 . Using this connection, the verifying device 130 can control access to and/or operations of the devices 210, 220, 230, 240. Of course the verifying device 130 could also be connected to a great variety of other devices, such as telephone booths, vending machines, Internet access terminals or toys.

The connection between the verifying device 130 and the devices 210, 220, 230, 240 can be wired or wireless, depending on what kind of device verifying device 130 is connected to. In Fig. 2, the connection with the gaming device 220 and the cash register 240 is wireless, and the connection with the devices 210 and 230 is wired. The verifying device 130 can also be embodied as a component installed inside the devices 210, 220, 230, 240.

When an authorization code is extracted from the watermarked signal 120, the access control module 133 checks whether the authorization code is applicable for any of the resources to which is connected: If this is not the case, the authorization code is ignored. Otherwise the access control module 133 performs an action appropriate for the authorization code and the resource to which the code applies. This will now be illustrated using various exemplary, non-limiting embodiments.

In a first example, the resource comprises a computer program 231 to be executed on the personal computer 230. The verifying device 130 is now preferably realized as a computer program running on the personal computer 230, although it could also be realized as one or more hardware modules installed in the personal computer 230, or as a separate device like in Fig. 2. Embodying the verifying device 130 as a part of the personal computer 230 has the advantage that components like the microphone 131 can be omitted, as they are usually present in the personal computer 230 already.

The authorization code now represents a license code granting permission for executing the computer program 231. By itself it is known in the field of computer software that execution of programs can be controlled using so-called license managers. License managers are computer programs that control the execution of other programs based on license codes. These known techniques can be adapted to work with the invention by supplying the authorization code to the license manager, which will subsequently allow a user to execute the computer program 231 based on the authorization code.

In a related embodiment, the computer program 231 is a so-called "shareware" application, in which certain modules providing certain functionality are disabled until the user supplies an authorization code. Usually the authorization code is supplied by the creator

of the program after the user makes a payment. In accordance with the invention, the authorization code is embedded in the watermarked signal 120, which preferably is a commercial for the computer program 231.

Another example involves the gaming device 220. This device 220 could be a hand-held gaming console, an arcade game machine or a computer program running on a general purpose or specially adapted computer. Of course the gaming device 220 usually operates essentially in the same way as the personal computer 230, so the license codes could also be supplied to the gaming device 220 to enable execution of particular games, or to allow access to certain parts of a game (which are modules of the game software). For example, extra "levels" in the game could be made available.

Many electronic games have so-called "cheat functions". Using these functions a player could for example easily get extra weapons or other objects for use in the game, earn extra points, walk through walls, get access to a map of the entire gaming environment, and so on. Typically the code necessary to activate a cheat function is supplied by pressing a specific sequence on a keyboard and/or operating a joystick in a particular way. In accordance with the invention, this code is supplied by the verifying device 130.

One particularly useful extension of this example involves television programs that discuss and/or review electronic games. A popular feature in such programs is providing cheat codes. In prior art systems this is done by verbally or graphically listing the keyboard sequences necessary to activate the cheat function. However, the invention makes it possible to embed the cheat code in the television program at the appropriate moment, so that the verifying device 130 can pick up the signal, extract the cheat code and supply the extracted code to the gaming device 220.

If the verifying device 130 is embodied as a part of the gaming device 220, then a player wishing to obtain a cheat code merely needs to watch the television program and use his gaming device 220 to pick up the signal when the cheat codes are being supplied. The gaming device 220 will then automatically detect the cheat codes.

Another useful application of the method according to the invention allows controlling access to copy protected multimedia objects like music, movies and so on. A digital rights management (DRM) system installed in the content playback apparatus 210 enforces restrictions on copying and/or playback of multimedia objects 212 e.g. stored in storage medium 211. These restrictions can be provided by embedding them in the multimedia objects using watermarking technology. For example, a multimedia object 213

could be made available for free on a web site, with the restriction that it can only be played back during the next week embedded in the object 213.

If a user attempts to play back that multimedia object 213 after that time period, the DRM system prohibits this. From that moment on the user must obtain authorization for playback in some other fashion, usually by buying a playback right from the copyright holder. In accordance with the invention, the authorization code comprises such a playback right. For example, if a radio station to which the user is listening broadcasts a specimen of the multimedia object 213, a one-time playback right could be embedded in the broadcast signal. The verifying device 130 picks up the one-time playback right and supplies it to the DRM system, so that the user gets an opportunity to play back the multimedia object 213 once.

This approach can, next to playback rights, also be used for copying rights. This allows the user to make a copy of a multimedia object when a signal comprising the appropriate authentication code is broadcast or transmitted to him otherwise.

Preferably the signal comprises an advertisement related to the multimedia object. For example, a record label might release a compact disc with a number of songs by one particular artist or group. To promote this release, advertisements are transmitted over radio and TV channels. The potential audience for this release most likely already has several multimedia objects comprising particular songs in its possession. By granting a one time playback right embedded in the advertisement, the record label encourages its potential audience to listen to its advertisements and whets the appetite for the compact disc because the audience will use the playback right to listen to the particular songs in its possession, and so become excited about the artist.

The verifying device 130 can also be connected to the cash register 240. The authorization code in that case preferably grants permission to the cash register 240 for applying a discount to a purchase being effected using the cash register 240. Using this embodiment an advertiser could easily offer discounts on his products by embedding discount codes into the watermarked signal 120. Consumers can pick up the watermarked signal 120 using the verifying device 130 and supply the extracted authorization code at a store to a sales clerk operating the cash register 240. The clerk subsequently enters the authorization code into the cash register 240, so that the discount is applied to the price of the product.

In this embodiment it may be advantageous to fit the verifying device 130 with the display on which the access control module 133 can display the authorization code.

Alternatively, using a wired or wireless connection (for example using Bluetooth) the access control module 133 could feed the authorization code directly to the cash register 240.

Preferably the permission is limited in time. This can be realized by adding a timestamp to the authorization code. A timestamp usually indicates the time at which the permission becomes valid, and/or the time at which the permission ceases to be valid. Alternatively, the timestamp could comprises a time period during which the permission is valid.

If the access control module 133 detects that a timestamp was added to the authorization code, it compares the timestamp against the current time as measured in the verifying device 130. This may require the installation of a real-time clock in the verifying device 130. If the current time exceeds the latest time at which the permission is valid according to the timestamp, the authorization code is rejected as invalid because it has expired.

The authorization code alternatively comprises an indication that a previously granted permission is to be revoked. The access control module 133 then revokes this permission. In the example involving computer program 231, this could be realized by signaling to the license manager that the license code for the computer program 231 is to be deleted, revoked or disabled.

Access control module 133 could also keep track of the time at which an authorization code was received, and automatically revoke a permission granted by an authorization code if the current time exceeds a certain amount of time after the time at which the code was received. If the authorization code comprises a timestamp indicating the end of the validity period, the access control module 133 automatically revokes the permission when the time indicated in the timestamp is reached.

It is to be expected that users will try to avoid receiving authorization codes that revoke previously granted permissions. One way to overcome this problem is to provide a positive authorization together with the revocation. For example, if the authorization code revokes permission to execute a beta or test version of a computer program, it could at the same time grant permission to execute the official release version of that computer program. This way a beta tester is encouraged to allow revocation of the beta version. Preferably this further authorization is delayed until a predetermined time has elapsed after the revocation took place.

It should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be able to design many alternative

embodiments without departing from the scope of the appended claims. For example, multiple authorization codes could be embedded in one or multiple watermarks in the signal. Next to an authorization code embedded in a signal using a watermark, additional codes could be provided in other channels, such as by using audible signals, by providing them in a Teletext channel, or visually showing them in a video signal or in an image. Different verifying devices could authorize different operations based on one authorization code in one signal received by both.

Rather than, or in addition to, being limited in time, the authorization can also be limited in space. This can be realized by e.g. adding an address on a computer network (like an IP address or hostname) to the authorization code, or by including Global Positioning System coordinates in the authorization code. The authorization code can also contain one or more other properties of the verifying device 130 to limit the scope of the authorization.

If the authorizations are limited in time, it becomes possible to require owners of the device 140 to periodically expose themselves to content with new authorizations. For instance, a toy could be given away for free with an initial authorization in place that is limited in time (say, a week). After that, the owner of the toy must periodically visit a location in which the device 114 is installed, preferably a fast food restaurant or toy store. The signal 120 produced by the device 114 grants the toy a new time-limited authorization so it operates for another week. If the owner does not visit the location every week, the toy ceases functioning or limits its abilities.

In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. The word "comprising" does not exclude the presence of elements or steps other than those listed in a claim. The word "a" or "an" preceding an element does not exclude the presence of a plurality of such elements.

The invention can be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer. In the device claim enumerating several means, several of these means can be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

CLAIMS:

1. A method of controlling access to a resource (140), comprising embedding an authorization code in a signal (120) by means of a watermark and transmitting the watermarked signal (120) to a verifying device (130), and in the verifying device (130), extracting the authorization code from the watermarked signal (120) and authorizing an operation to be performed on the resource (140) in dependence on the extracted authorization code.

2. The method of claim 1, in which the resource (140) comprises a computer program and the authorization code causes the verifying device (130) to grant permission for executing the program.

3. The method of claim 1, in which the resource (140) comprises a computer program and the authorization code causes the verifying device (130) to grant permission for activating a module of the computer program.

4. The method of claim 1, in which the resource (140) comprises an electronic game and the authorization code causes the verifying device (130) to grant permission for activating a cheat function in the electronic game.

5. The method of claim 1, in which the resource (140) comprises a multimedia object and the authorization code causes the verifying device (130) to grant permission for at least one of: a rendering of the multimedia object and the making of a copy of the multimedia object.

6. The method of claims 2, 3, 4 or 5, in which the permission is limited in time.

7. The method of claim 1, in which the resource (140) comprises a computer program and the authorization code causes the verifying device (130) to revoke a previously granted permission for executing the program.

8. The method of claim 7, in which the authorization code further causes the verifying device (130) to authorize a further operation to be performed on the resource.

9. The method of claim 1, in which the signal (120) comprises an advertisement related to the resource (140).

10. A verifying device (130) arranged for controlling access to a resource (140), comprising receiving means (131) for receiving a watermarked signal (120), watermark detection means (132) for detecting an authorization code embedded in the watermarked signal (120), and access control means (133) for authorizing an operation to be performed on the resource (140) in dependence on the extracted authorization code.

11. The verifying device (130) of claim 10, in which the authorization code comprises a timestamp and the access control means (133) are arranged for authorizing the operation further in dependence on a comparison of the timestamp against a current time.

12. A computer program product arranged for causing a general purpose computer to function as the verifying device (130) of claim 9.

13. A signal (120) in which an authorization code is embedded by means of a watermark.

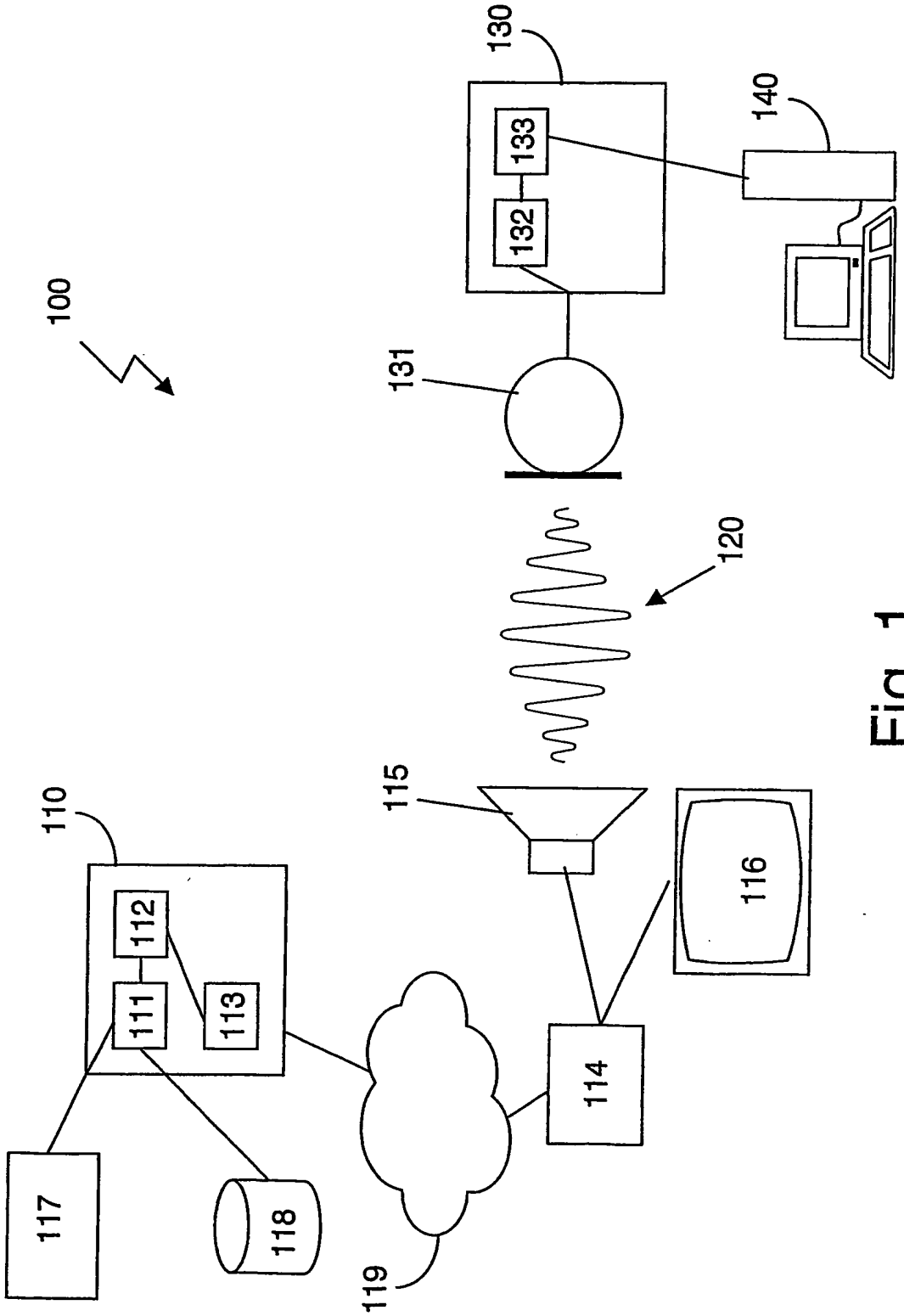

100
110
111
112
113
114
115
116
117
118
119
120
130
131
132
133
140

Fig. 1

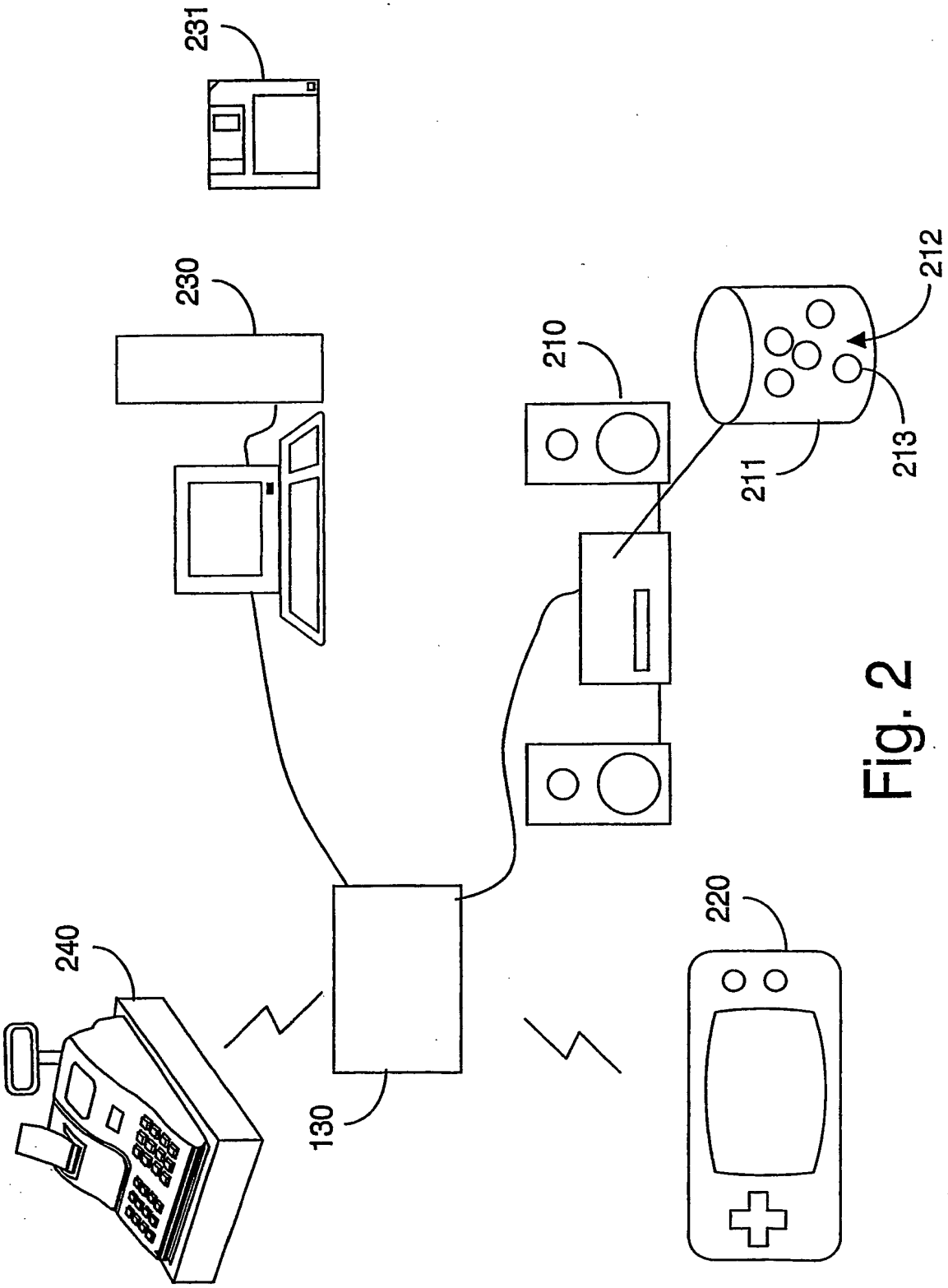



Fig. 2